基于匹配追逐的视频压缩加密方案

侯会满 张 荣 李卫海 邵肖伟
(中国科学技术大学电子工程与信息科学系多媒体计算与通信教育部-微软重点实验室, 合肥 230027)

摘 要 加密是视频安全传输的关键技术之一。通常视频加密是在一定的压缩框架下进行加密,由于变换后系数分布一般都具有一定的统计特性,而对变换系数进行完全置乱就会破坏这些特性,导致比特率增加。从便于加密的角度出发,联合考虑视频的压缩和加密,提出一种基于匹配追逐(matching pursuit)的视频压缩加密方案,该方案首先构造基于匹配追逐的视频压缩平台,由于视频信号经匹配追逐分解后,其分解系数的分布取决于字典的选取和输入信号空间特性,即变换系数的分布是随机的,再对变换系数进行完全加密,提高数据的安全性而不会改变压缩效率。实验结果证明了该方案的有效性。

关键词 视频加密 匹配追逐 安全性分析
中图法分类号: TN918.74 **文献标识码**: A **文章编号**: 1006-8961(2007)05-0831-05

A Scheme of Video Compression and Encryption Using Matching Pursuit

HOU Hui-man, ZHANG Rong, LI Wei-hai, SHAO Xiao-wei
(*Department of Electronic and Engineering and Information Science, MOE-Microsoft Key Laboratory of Multimedia Computing and Communication, University of Science and Technology of China, Hefei* 230027)

Abstract Encryption is one of the key techniques of video security. Usually video encryption is based on a given compression scheme. Scrambling the transform coefficients will change the statistical characteristics and result in the increase of the bit rate of the compressed video. In the view of encryption, this paper proposes a union coding scheme for compression and encryption based on the matching pursuit(MP). On the compression platform based on this method, the decomposed coefficients are of random distribution. The complete scrambling will not increase the bit rate, but with higher security. Experimental results are given to demonstrate the efficiency of this method.

Keywords video encryption, matching pursuit, security analysis

1 引 言

近年来,数字视频技术迅猛发展,各种应用层出不穷:从视频会议(video conference)到视频点播(vidio of VOD),从数字电视到多视点电视(multi-view TV)。可以预见,在不久的将来,数字视频一定会应用于多种行业,走进千家万户。同时,一个新的问题随之而来:如何保证只有已付费的或已授权的用户才可以接受指定质量的数字视频服务?即视频加密问题。由于视频信号的数据量巨大,而网络带宽有限,因此视频总是以压缩的形式进行传播的。这样,就需要结合压缩平台来设计加密方案,一方面要使加密后的数据与解压格式兼容,另一方面要保证数据的有效传输。

现有的视频加密技术大致可以分两类:(1)针对现有压缩标准(如 MPEG-2, MPEG-4, H.263, H.264 等)进行选择性加密。这些压缩标准以离散

基金项目:多媒体计算与通信教育部-微软重点实验室科研基金项目(05071802)
收稿日期:2006-01-06;改回日期:2006-02-23
第一作者简介:侯会满(1981 ~),男。中国科学技术大学电子工程与信息科学系硕士研究生。主要研究方向为基于匹配追逐算法的视频压缩和视频加密、图像处理。E-mail:hmhou@mail.ustc.edu.cn

余弦变换(discrete cosine transform, DCT)为核心,其基本框架为:视频数据→运动补偿→DCT 变换→量化→zig-zag 排序→熵编码,针对压缩步骤中的每一步进行数据置乱(scrambling)都可以实现加密。如 Tang 等人提出 DCT 系数洗牌(shuffling)的方法[1],能提供一定水平的安全性,但由于改变了 DCT 系数分布的 zig-zag 特性,从而增加了 50% 的比特率(bit rate)。为了保证比特率,很多方法采用选择性加密[2~4],例如只加密 I 帧、加密每个 DCT 系数的符号位、置乱 P/B 帧中含帧间编码块的段(slice)、加密运动矢量的符号位、置乱一段中的运动矢量、对熵编码中 Huffman 表加密等等,或多种方法联合使用;(2)基于小波变换的压缩框架[5,6],用小波变换取代 DCT 变换,加密方式包括:①对小波变换系数的符号位置乱;②把每个子带分块,不同子带的块用不同的表进行洗牌;③由密钥控制块进行旋转;④用小波包分解视频数据,对所选滤波器进行置乱等等。由于小波变换本身的多分辨率特性,这一类方法加密压缩后的码流具有空间可伸缩特性(spatial scalability)。

上述方法都是基于这样一个前提:变换后的系数分布具有一定的统计特性(如 DCT 中的 zig-zag 特性,小波变换中零树特性等),针对这些特性,设计特定的编码器以提高压缩效率,加密则通过对变换后的系数进行选择性置乱来实现。因为对变换后的系数进行完全置乱会破坏这种统计特性,导致比特率增加,所以为了保证比特率,同时又要在压缩过程中完成加密,就只能选择部分系数加密,使安全性降低,从而导致了压缩效率与安全性之间的矛盾。可见上述方法都是在压缩效率和安全性之间的折中。

针对这一矛盾,设计出一种基于匹配追逐的视频压缩加密方案,使得对变化系数进行完全置乱也不会影响压缩效率,通过对变换系数进行完全加密,提高视频数据的安全性,解决了压缩效率与安全性之间的矛盾。匹配追逐也是一种变换,它取代 DCT 变换或小波变换,用超完备基对信号能量进行分解,分解得到的系数不存在统计特性,因而可以随意置乱。与其他变换相比,匹配追逐的特点可以总结为:(1)用超完备基表示信号,可以用少量的基表示给定质量的信号;(2)最先分解出信号最重要的部分,这使得它适用于数据压缩,尤其适合低比特率压缩;(3)变换后系数的分布取决于基函数的选取和输入信号空间特性,即变换后系数的分布是随机的,并不存在 DCT 变换中的 zig-zag 特性,或者小波变换中零树特性。因此对变换后系数的加密从理论上不会影响压缩效率,即完全加密不会降低压缩效率,这一点使它非常适合用于加密,以提高视频数据的安全性。

实验中,本文建立了一个基于匹配追逐的压缩平台,通过实验验证了匹配追逐的压缩效率后,再对匹配结果的系数进行加密。实验结果表明:基于匹配追逐的视频加密方案对码率没有影响,同时加密算法简单、安全性较好。

2 匹配追逐算法

匹配追逐算法[7]最早由 Mallat 和 Zhang 于 1993 年提出,这种方法借鉴了传统的投影追逐算法(projection pursuit)的思想,并将其近一步完善,以作为一种时频分析的手段。简单的说,匹配追逐算法就是将信号在一组基上以能量最大为准则的分解过程,这一点不同于 DCT 变换或小波变换每次的分解是按照特定的顺序进行,因此匹配追逐分解出的系数不具有 DCT 变换或小波变换那样的统计特性。即 $f(t) = \sum_{n=0}^{+\infty} a_n g_{\gamma_n}(t)$,其中令 $\boldsymbol{D} = \{g_\gamma\}$ 为一组时频基(称为字典),并满足以能量最大的准则下按 $a_n g_{\gamma_n}(t)$ 的重要性递减。

要构造一组时频基,可以通过对一个简单的窗函数 $g(t)$ 进行平移、缩放和调制来得到。假定 $g(t)$ 是实函数、连续可导,并且 $\|g(t)\| = 1$。令 $\gamma = (s,u,\xi)$,其中 s 代表尺度变换,u 代表平移,ξ 代表调制,则

$$g_\gamma(t) = \frac{1}{\sqrt{s}} g\left(\frac{t-u}{s}\right) e^{i\xi t} \tag{1}$$

通过取 N 个不同的 (s,u,ξ) 值来获得一组时频基 $g_{\gamma_i}(t)$,$i = 0,1,\cdots,N-1$。其中,N 为基的维数,相应的 (s_i,u_i,ξ_i) 就是每一个基的参数。

有了这组时频基(字典),就可以把信号 $f(t)$ 分解为

$$f(t) = \sum_{n=0}^{+\infty} a_n g_{\gamma_{m[n]}}(t) \tag{2}$$

其中,$m[n] \in (0,N-1)$,表示第 n 次匹配用到的基的代号,

$$a_n = \langle f, g_{\gamma_{m[n]}} \rangle \tag{3}$$

$\langle \cdot \rangle$ 为内积运算,a_n 满足重要性递减。a_n 以迭代方

式求解:记 R_f 为 f 去除在 g_γ 上投影的残余分量,则 $f=\langle f,g_\gamma\rangle g_\gamma+R_f$,$a_n$ 为 f 在各个基上最大的投影值,即 $a_n>(\langle f,g_{\gamma_i}\rangle)$,$i\neq m[n]$ 和 $i\in(0,N-1)$;再将残余分量 R_f 在原有基张成的空间中分解,即得到下一个分解系数 a_{n+1};重复该过程直到 $f(t)$ 达到收敛的要求或是匹配次数达到迭代次数的上限。这样就把信号 $f(t)$ 投影到了构造的一组基 $g_{\gamma_i}(t)$ 上,而 a_i 和 $m[i]$ 将作为匹配的结果,用来重建信号 $f(t)$。

采用 Gabor 函数时作为窗函数。Gabor 函数可以定义为:$g(t)=\sqrt[4]{2}e^{-\pi t^2}$,由于 Gabor 函数满足作为窗函数的条件而且便于调制,因此将它作为窗函数 $g(t)$ 来构造时频基。定义一组不同频率、长度、相位的 Gabor 集[8] $G=\{g_\alpha(i)\}$,其中

$$g_\alpha(i)=K_\alpha\cdot g\left(\frac{i-\frac{N}{2}+1}{s}\right)\cdot\cos\left(\frac{2\pi\xi\left(i-\frac{N}{2}+1\right)}{16}+\varphi\right)$$
$$i\in\{0,1,\cdots,N-1\}\qquad(4)$$

其中,N 为每个基中含有的离散点的个数,即每个基的长度。

此处 $\alpha=(s,\xi,\varphi)$ 为一向量,其中,s,ξ,φ 分别代表了该 Gabor 函数的尺度、频率和相移。K_α 是归一化常数。2 维 Gabor 函数可以由两个 1 维基函数相乘得到:

$$g_{\alpha,\beta}(i,j)=g_\alpha(i)\cdot g_\beta(j)\qquad(5)$$
$$i,j\in\{0,1,\cdots,N-1\}$$

这样就构造了一组 2 维 Gabor 基,本文将用它来对视频残差信号进行分解。

3　视频压缩加密方案

视频编码的对象是以帧为单位的图像信息,图像作为一种 2 维数据,需要使用 2 维基来进行匹配追逐。首先采用传统的视频编码方案中的运动估计减少帧间冗余,将帧分为 I 帧,P 帧和 B 帧 3 种。由于匹配追逐按能量大小进行分解,对于能量大的图像分解次数较多,分解速度慢,因此对于 I 帧(能量大)仍采用基于 DCT 的方法进行压缩和加密,对 P 帧和 B 帧则采用匹配追逐方法进行压缩和加密(通过置乱匹配追逐后得到的编码数据来实现加密)。图 1 为该视频加密方案的编码器框图。

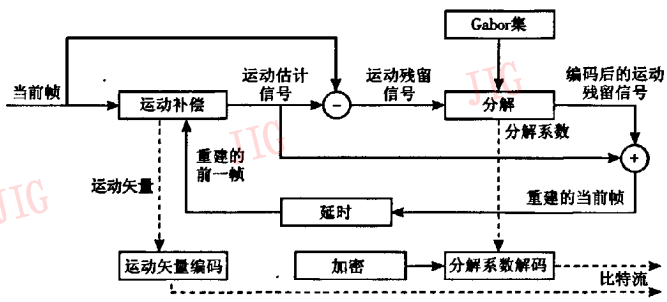


图 1　匹配追逐视频加密方案编码器模型

Fig. 1　The model of MP video encryption encoder

该方案编码流程中的几个核心步骤如下。

3.1　分解系数

虽然匹配追逐对整幅残差图像进行分解会最先找到整幅残差图像中能量最大的部分,但是这样做计算量和对存储器的需求都是十分巨大的。将整幅残差图像分块并在块内匹配就可以减少很多计算。因此在实验中,将整幅残差图像分成 16×16 的小块,计算每个块自身所包含信息的能量,找到能量最大的块(该过程称为能量搜索)。然后在该块内进行匹配追逐:以块内区域作为候选区域,将一组(20×20 个)2 维 Gabor 基的中每一个基逐个对其做内积,选择内积最大的基来得到一个分解元素,每个元素可以由 5 个参数决定,它们分别是:最匹配基的 2 维代号(N_x,N_y);最匹配基的块内位置(x,y);最匹配基与相应位置上图像数据的内积 P。

在这个块得到一个匹配结果之后,残差图像减去匹配结果就得到分解一次之后的残差图像,对新的残差图像再重复能量搜索的过程,找到能量最大的块,然后在这个块中重复上述过程,直到达到所要求的匹配次数。如果连续两次找到的能量最大的块是同一个块,则只要把原来计算得到的所有内积减去与上一个匹配结果内积相关的部分,就可以省去

重复的计算。匹配次数取决于码速率。码速率越高,匹配次数越多;反之越少。

3.2 系数编码

对匹配追逐的结果进行编码时,以块为单位首先写入该块中进行匹配追逐的元素的个数,然后分别写入该块内每个元素的信息:其中 N_x , N_y,x,y 采用 Huffman 编码,匹配内积则先做量化然后采用定长编码。

3.3 加密

在对视频数据的压缩加密中,对于 I 帧实验中采用了 DCT 的编码方案。其中的加密方法采用运动矢量加密与符号翻盘加密的结合。P 帧和 B 帧用匹配追逐方法编码,采用对基的代号和位置进行置乱的方法进行加密,由于 Huffman 编码与每个基的排列次序无关,所以置乱不会影响码率的大小。置乱的范围可以将几个元素作为一组来改变,也可以对所有元素一起置乱。

在一个 16×16 的块内,假设匹配追逐得到 16 个分解元素,然后置乱这 16 个元素的字典代号,再置乱他们的位置代号,那么加密空间[6]为 16!×16!,在没有密钥的情况下要计算约 10^{26} ~ 10^{27} 次才能解密。

4 实验结果

根据图 1 所示的框架,搭建一个基于匹配追逐算法的实验平台和一个基于 DCT 方法的平台与之比较。两个实验平台具有完全相同的运动估计方法和 I 帧编码方法(DCT 方法),唯一的区别在于对运动估计后的残差处理上,一个用匹配追逐方法,一个用 DCT 方法。加密前两者性能比较如表 1所示。

表 1 匹配追逐(MP)方法与 DCT 方法性能比较

Tab.1 The comparison of MP method and DCT method

视频序列	编码方案	码速率(kbps)	*PSNR_Y*(dB)	*PSNR_U*(dB)	*PSNR_V*(dB)
Bus_qcif	DCT	182.34	28.63	37.16	37.46
	MP	185.28	28.53	36.78	37.14
Bus_qcif	DCT	147.68	27.64	36.63	37.22
	MP	149.02	27.47	36.39	36.91
Foreman_qcif	DCT	70.728	32.15	36.71	37.73
	MP	72.125	32.07	35.43	36.85
Foreman_qcif	DCT	54.62	31.06	35.86	36.96
	MP	54.79	31.02	35.28	36.23

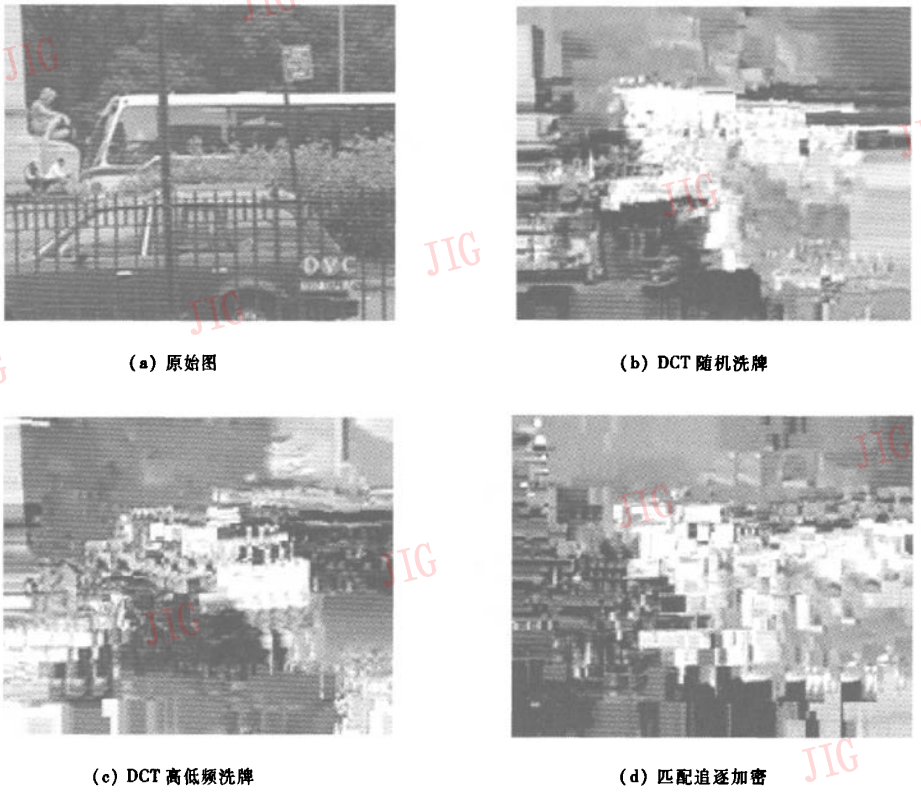
可见,基于匹配追逐的视频压缩方案具有与 DCT 方案相近的压缩效率。对标准序列 Bus_qcif 进行加密测试,每隔 15 帧编码一个 I 帧,在编码前 30 帧的情况下对如下性能进行了比较,实验结果如表 2所示。

实验结果说明,基于 DCT 压缩框架的加密随着安全性的提高,编码效率不断降低。而匹配追逐加密后对码速率没有影响,这充分证明采用匹配追逐算法的加密方法更满足对加密性能的要求,而加密的主观效果相当,如图 2 所示。

表 2 不同加密方法的性能比较

Tab.2 The comparison of different encryption methods

	DCT			匹配追逐	
	加密前	加密后		加密前	加密后
		随机洗牌	高低频洗牌		
码速率(kbps)	147.68	154.87	167.80	149.05	149.05
加密空间(仅一个宏块内)		16!	16×16!		16!×16!
加密空间近似值		10^{13} ~ 10^{14}	10^{14} ~ 10^{15}		10^{26} ~ 10^{27}



(a) 原始图　　(b) DCT 随机洗牌

(c) DCT 高低频洗牌　　(d) 匹配追逐加密

图 2　Bus_qcif. yuv 第 11 帧加密效果比较

Fig. 2　The comparison of Bus_qcif. yuv frame 11's encryption effect

5　结论和展望

本文提出了一套完整的基于匹配追逐的视频压缩加密方案。由于匹配追逐的分解方式使得加密对码速率没有影响,通过在实验中与几种基于 DCT 的加密算法进行比较,可以看出匹配追逐算法应用于视频加密的独特优势:安全性好、对编码性能没有影响。这些性能表明这种方案有利于视频的安全传输和应用。

参考文献(References)

1　Tang Lei. Methods for encrypting and decrypting MPEG video data efficiently[A]. In: Proceedings of the Fourth ACM International Multimedia Conference(ACM Multimedia'96)[C], Boston, MA, USA, 1996: 219 ~ 229.

2　Zeng Wenjun, Lei Shawmin. Efficient frequency domain selective scrambling of digital video[J]. IEEE Transactions on Multimedia, 2003, 5(1): 118 ~ 129.

3　Li W. Overview of fine granularity scalability in MPEG-4 video standard[J]. IEEE Transactions on Circuits and System for Video Technology, 2001, 11(3): 301 ~ 317.

4　Can Xiao-ying, Sun Shi-ying, Song Wen-tao. A new encryption algorithm for digital video based on pseudo-random sequence[J]. Journal of Data Acquisition and Processing, 2002, 17(3): 248 ~ 251.[甘小莺,孙诗瑛,宋文涛. 基于伪随机序列的视频图象加密新算法[J]. 数据采集与处理, 2002, 17(3): 248 ~ 251.]

5　Wee S J, Apostolopoulos J G. Secure scalable streaming enabling transcoding without decryption[A]. In: Proceedings of 2001 International Conference on Image Processing[C], Thessaloniki, Greece, 2001: 437 ~ 440.

6　Lian Shi-guo, Sun Jin-sheng, Wang Zhi-quan. Quality analysis of several typical MPEG video encryption algorithms[J]. Journal of Image and Graphics, 2004, 9(4): 483 ~ 490.[廉士国,孙金生,王执铨. 几种典型视频加密算法的性能评价[J]. 中国图象图形学报, 2004, 9(4): 483 ~ 490.]

7　Mallat S, Zhang Z. Matching pursuits with time-frequency dictionaries[J]. IEEE Transactions on Signal Processing, 1993, 41(12): 3397 ~ 3415.

8　Neff R, Zakhor A. Matching pursuit video coding. I. Dictionary approximation[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2002, 12(1): 13 ~ 26.